

Using PGP TrustCenter's Digital Certificates with Microsoft Office 2007

To use any of the security features in Microsoft Office 2007, you must first obtain a digital certificate. If you do not already have a digital certificate, please visit PGP TrustCenter's website at <http://www.pgptrustcenter.com/digital-certificate-solutions> to obtain a "TC Personal ID" or "TC Business ID".

About Digital Signatures

You can digitally sign a document for many of the same reasons you might sign a paper document. A digital signature is used to authenticate digital information — such as documents, e-mail messages, and macros — by using computer cryptography. Digital signatures help to establish the following assurances:

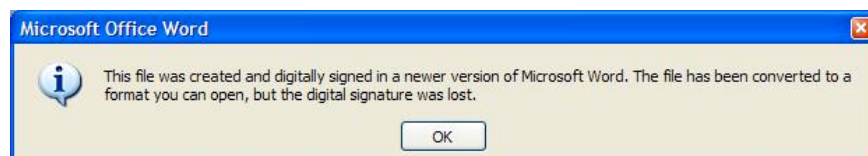
- **Authenticity:** The digital signature helps to assure that the signer is who he or she claims to be.
- **Integrity:** The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation:** The digital signature helps to prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content.

To make these assurances, the content creator must digitally sign the content by using a signature that satisfies the following criteria:

- The digital signature is valid (legitimate, current, and not expired or revoked).
- The certificate associated with the digital signature is current (not expired).
- The signing person or organization, known as the publisher, is trusted.
- The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA) such as PGP TrustCenter.

Compatibility Issues

Microsoft Office 2007, unlike its predecessors, uses the XMLDSig format for digital signatures. It is important to note that digital signatures are not compatible across Microsoft Office platforms. For example, if a document is signed using Microsoft Office 2007 and opened in a Microsoft Office 2003 application with the Office Compatibility Pack installed, the user will be informed that the document was signed by a newer version of Microsoft Office and the digital signature will be lost, as seen in the below screen shot:



Warning that the digital signature is moved when opened in an earlier version of Office

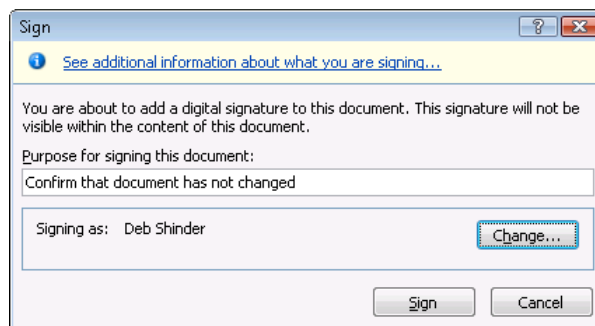
Digitally Signing Office 2007 Documents

After you have your digital certificate with private keys installed, you can digitally sign your office applications, such as Word, Excel and PowerPoint. Office 2007 allows for two types of digital signatures to be applied to documents, spreadsheets and presentations:

1. **Transparent or Invisible Digital Signatures:** No visible signature lines are present within the document, but the document is digitally signed to provide assurance as to authenticity, integrity and origin of the document.
2. **Digital Signature Lines:** One or more visible signature lines are inserted within the document which allows for a visible signature to be tied to a digital signature.

1. To add an Invisible Digital Signature, follow these steps:

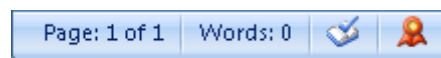
1. Click the **Office** button, **Prepare**, and then choose **Add a Digital Signature**.
2. You will see a Microsoft Office dialogue box. If you already have your digital certificate from PGP TrustCenter, just click **OK**. You may also check the box to "Don't show this message again".
3. If the document has not already been saved to the Office 2007 format, a message will ask you to save it first. Click **Yes** to save the document as a new format.
4. A **Sign** dialogue box will appear that defaults to use an appropriate signing certificate. If you have multiple certificates installed, and this is not the one that you wish to use, click on the **Change** button to select the correct certificate. In the **Purpose for signing this document** text box, you can enter a reason for signing or leave it blank. Click the **Sign** button when all values are correct.



5. The Signature Confirmation dialogue box appears. Click **OK** to proceed.

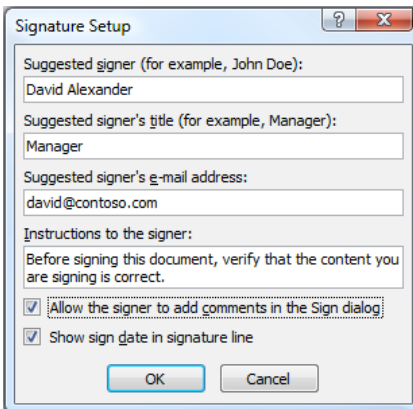


6. If there are no problems with the certificate, the document will now be signed. Note that if the certificate you are using was not issued from a trusted Certificate Authority, such as PGP TrustCenter's TC TrustCenter, a Signatures task pane will be displayed where you will need to correct any problems identified.
7. The digital signature is now apparent in the lower left-hand corner of the document where a red ribbon is displayed. You can click on the ribbon to display information about the signing certificate and purpose for signing the document.



2. To add one or more Visible Digital Signature Lines, follow these steps:

1. Click the **Insert** tab and then click the **Signature Line** button.
2. The **Signature Setup** dialogue box appears. Enter information about the **Suggested signer**, **Suggested signer's title**, and **Suggested signer's e-mail address**. Put a checkmark in the **Allow the signer to add comments to the Sign** dialogue if you want the signer to add additional information into the signature line, and put a checkmark in the **Show sign date in signature line** checkbox to add the date the document was signed in the text box. Click **OK**.




3. A digital signature line now appears in the document. Double click the signature line to provide more information.

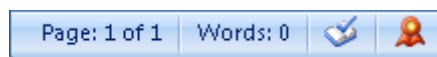
X

David Alexander
Manager

4. In the **Sign** dialogue box you can type your name, or if you have a tablet PC, you can write your name into the text box. If you don't have a tablet PC, but would like an image of your actual signature to be included in the signature line, you can click the **Select Image** link and insert a graphic file containing your handwritten signature.
5. In the **Select Signature Image** dialogue box, select the image of your signature and click the **Select** button.
6. The image now appears in the **Sign** dialogue box. Before signing the document, you can enter a reason for signing the document in the **Purpose for signing this document** text box. Click **Sign** to digitally sign the document.
7. If there are no problems with the certificate, the document will now be signed. Note that if the certificate you are using was not issued from a trusted Certificate Authority, such as PGP TrustCenter's TC TrustCenter, a Signatures task pane will be displayed where you will need to correct any problems identified.

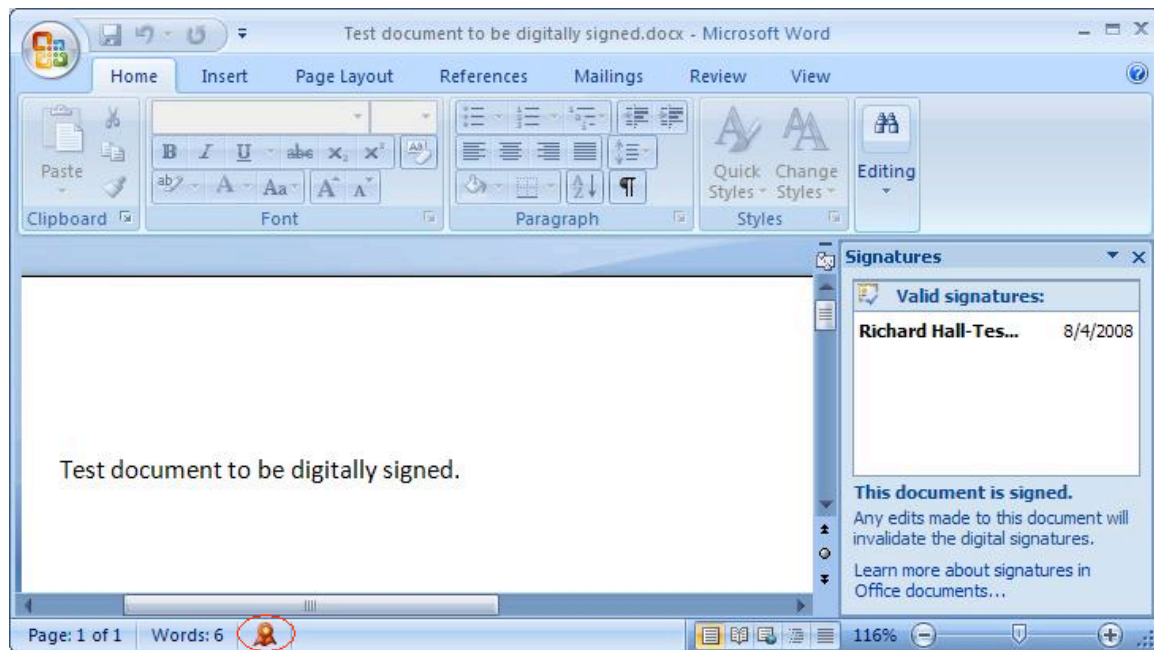
3/23/2007
X 
Deb Shinder
Manager

8. The digital signature is apparent in the lower left-hand corner of the document where a red ribbon is displayed. You can now click on the ribbon to display information about the signing certificate and purpose for signing the document.

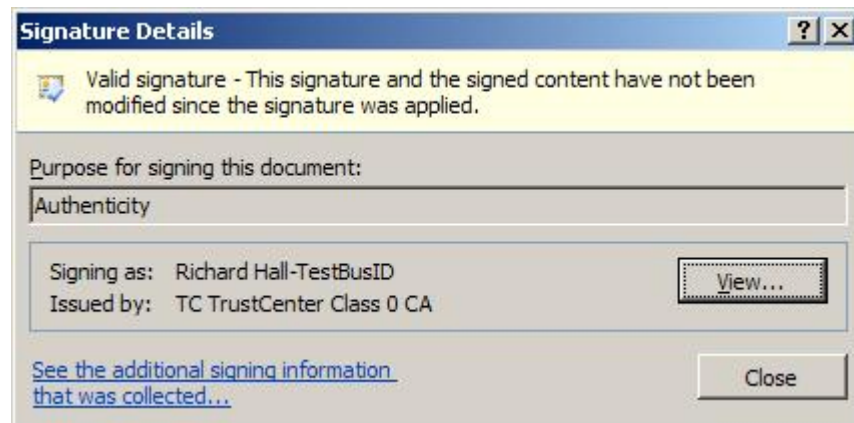


Verifying a Digitally Signed Document

When you open a digitally signed document, a red ribbon is displayed in the lower left-hand corner of the document.



A digitally signed document can be verified by clicking on the red certificate icon at the bottom of the document and then selecting the signature from the pane on the right-hand side of the document. This will display information about the signing certificate, the certificate's validity and the reason why the document was signed:



Clicking on the **View** button will display the signing certificate.

A digitally signed document cannot be modified in anyway, and if it is, the signature will be invalidated.


Digitally Signing Office 2007 Macro Projects

To digitally sign macro projects, you will need to obtain a "TC Publisher ID for Authenticode" code signing certificate which can be purchased online here:

<http://www.pgptrustcenter.com/tc-publisher-id-for-ms-authenticode>

To digitally sign macro projects, follow the steps below:

1. Open the file that contains the macro project you want to sign.
2. On the **Developer** tab, in the **Code** group, click **Visual Basic**.

If the **Developer** tab is not available, click the **Microsoft Office Button** , and then click **<Product> Options** for the associated product (Excel, Word, PowerPoint, etc.). Now click **Popular**, and then select the **Show Developer tab in the Ribbon** check box. Note: The Ribbon is part of the Microsoft Office Fluent user interface.

3. In the Visual Basic Project Explorer, select the project you want to sign.
4. On the **Tools** menu, click **Digital Signature**.
5. Do one of the following:
 - If you haven't previously selected a digital certificate or want to use another one, click **Choose**, select the certificate, and then click **OK** twice.
 - To use the current certificate, click **OK**.

Notes:

Sign macros only after your solution has been tested and is ready for distribution, because whenever code in a signed macro project is changed in any way, its digital signature is removed. However, if you have the valid digital certificate that was previously used to sign the project on your computer, the macro project is automatically re-signed when you save it.

If you want to prevent users of your solution from accidentally changing your macro project and invalidating your signature, lock the macro project before you sign it. Your digital signature says only that you guarantee that the project has not been tampered with since you signed it. Your digital signature does not prove that you wrote the project. Therefore, locking your macro project doesn't prevent another user from replacing the digital signature with another signature. Corporate administrators can re-sign templates (template: A file or files that contain the structure and tools for shaping such elements as the style and page layout of finished files. For example, Word templates can shape a single document, and FrontPage templates can shape an entire Web site.) and add-ins (add-in: A supplemental program that adds custom commands or custom features to Microsoft Office.) so that they can control exactly what users can run on their computers.

If you create an add-in that adds code to a macro project, your code should determine if the project is digitally signed and should notify the users of the consequences of changing a signed project before they continue.

When you digitally sign macros, it is important to obtain a timestamp so that other users can verify your signature even after the certificate used for the signature has expired. If you sign macros without a timestamp, the signature remains valid only for the validity period of your certificate.